Defense Security Service

# Risk Management Framework (RMF)

**August 2016**

# What is Risk Management Framework (RMF)

- It is a unified information security framework for the entire federal government that replaces legacy Certification and Accreditation (C&A) Processes applied to information systems
- RMF is a key component of an organization's information security program used in the overall management of organizational risk

# RMF Policy References

**NIST**

- SP 800-30
- SP 800-37
- SP 800-39
- SP 800-53
- SP 800-53A
- 800-137)

**CNSS**

- CNSSP 22
- CNNSI 1253
- CNSSI 1253A
- CNSSI 4009

**NISP**

- DoD 5220.22-M
- Industrial Security Letters
- DSS Assessment and Authorization Process Manual

# RMF Process Stakeholders: New Terminology

Many RMF stakeholder titles have been revised in the transition from C&A. The following table outlines former terms in the C&A process as well as the corresponding **new terms in the RMF process**. You may continue hearing both sets of terms during the transition to RMF.

| Old Term in the C&A Process | New Term in the RMF Process |
|---|---|
| Designated Approving Authority (DAA) | Authorizing Official (AO) |
| Regional Designated Approving Authority (RDAA) | Regional Authorizing Official (RAO) |
| Office of the Designated Approving Authority (ODAA) | NISP Authorization Office |
| Information System Security Professional (ISSP) | Security Control Assessor (SCA) |
| Customer, Government Contracting Activity (GCA) | Information Owner (IO) |
| Contractor | Information System Owner (ISO) |
| Information System Security Manager (ISSM) | ISSM |
| Information System Security Officer (ISSO) | ISSO |

**Titles will remain the same in RMF*.

# Connecting the Dots Old and New

| Process | C&A | RMF |
|---|---|---|
| ODAA Business Management System (OBMS) | same | same |
| SSP Template | same | same |
| Categorization | Basic, Med, High PLs | Low, Mod, High Accessibility |
| Certification Statement | same | same |
| Risk Acknowledgement/Tailoring-out | Risk Acknowledged | Tailored-Out/Risk Acknowledgement |
| MOU/Enhancements | MOU | MOU/ISA |
| Standing-Up Like System | Self-Certification | Type Authorization |
| Controls | NISPOM Refs | NIST Controls |
| Approval to Process | Accreditation | Authorization |

# Connecting the Dots Cont.

| Process | C&A | RMF |
|---|---|---|
| Submission<br>Validation within OBMS | SSP<br>Certification Statement<br>Profile | SSP<br>Certification Statement<br>POAM<br>Risk Assessment Report |
| | | |
| Assessment<br>Comments on issues | Comments Form | Security Assessment Report (SAR) |

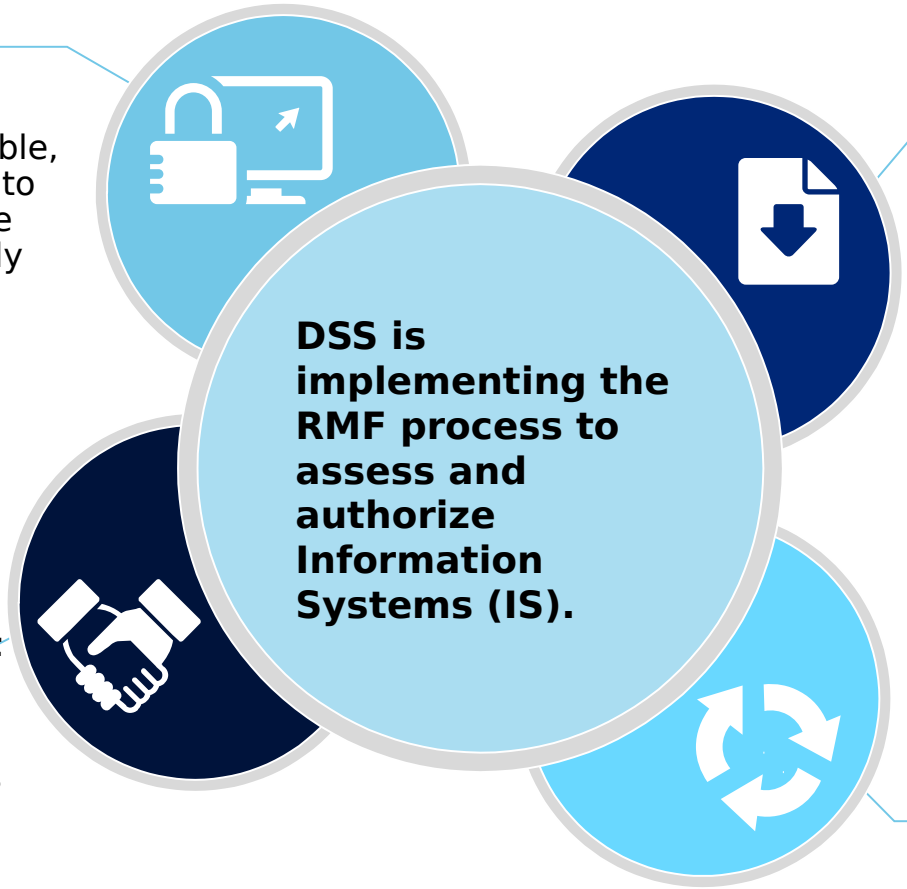
# Key Factors Driving the Transition to RMF

**Effective and Efficient Risk Management**

Shift from a static, "check-the-box" mentality to a flexible, dynamic approach to assess and manage risk more effectively and efficiently.

**Common Foundation for Information Security**

Implement a common foundation for information security that aligns to federal government standards for DSS and cleared contractors for a more uniform and consistent approach to manage risk associated with the operation of a classified IS.




**Trust Across the Federal Government**

Build reciprocity with other federal agencies to develop trust across the federal government through a more holistic, flexible, and strategic process for the risk management of IT systems.

**Streamline DSS processes**

Streamline DSS processes to support the authorization of a cleared contractor's IS processing classified information as part of the NISP.

# Roles and Responsibilities in the RMF Process

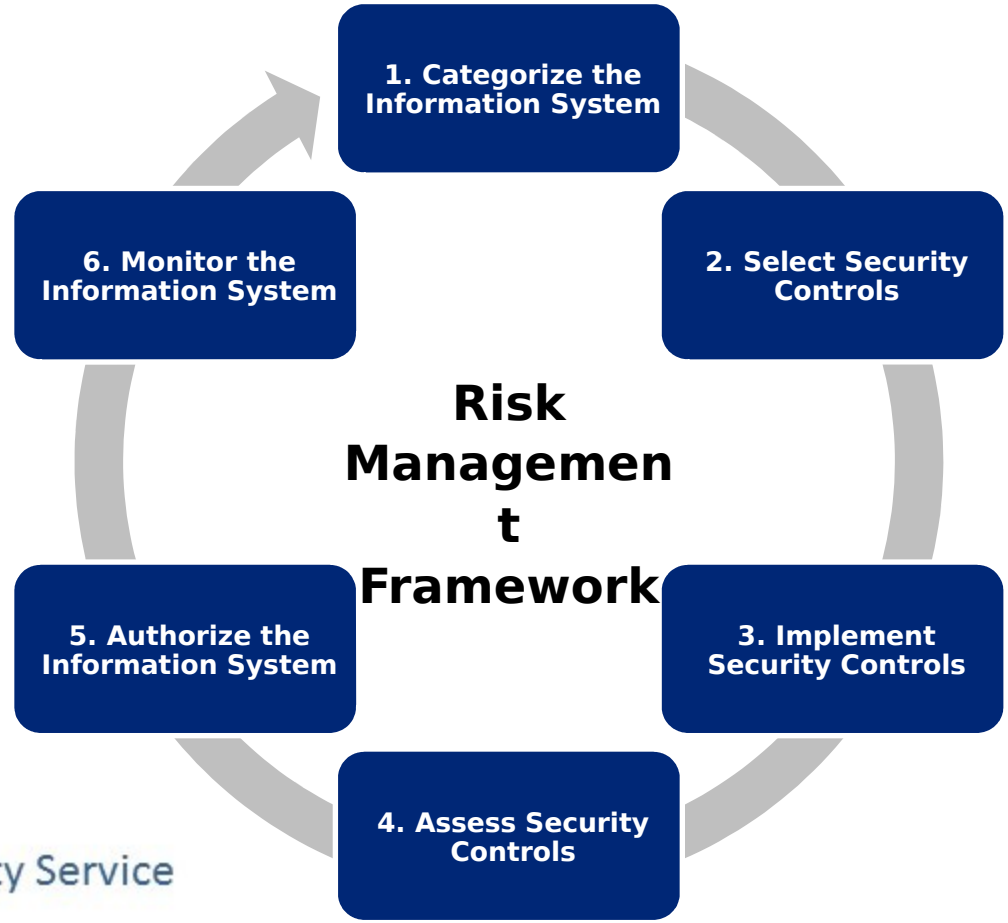
| Role | | Responsibilities |
|---|---|---|
| | **Authorizing Official (AO) (formerly the DAA) and Designated Authorizing Official (DAO) (formerly the RDAA)** | • Formally assumes responsibility for operating an IS at an acceptable level of risk to organizational operations, organizational assets, individuals, other organizations, and national security |
| | **Security Control Assessor (SCA) (formerly the ISSP)** | • Performs oversight of a contractor's IS processing classified information<br>• Conducts a comprehensive assessment of the management, operational, and technical security controls employed within or inherited by an IS to determine the overall effectiveness of the controls<br>• Provides an assessment of the severity of weaknesses or deficiencies discovered in the IS and its environment of operation and recommends corrective actions<br>• Provides an authorization decision recommendation to the DAO |
| | **Common Control Provider (CCP) (formerly the Host "Node")** | • Assumes responsibility for the development, implementation, assessment, and monitoring of common security controls |
| | **Information Owner (IO)/Government Contracting Activity (GCA) (a.k.a. the Customer)** | • Holds statutory, management, or operational authority for specific information to establish the policies and procedures governing its generation, collection, processing, dissemination, and disposal<br>• Establishes the rules for appropriate use and protection of the subject information and retains that responsibility when the information is shared with or provided to other organizations<br>• Provides input to the Information System Owners (ISOs) regarding data |

# Roles and Responsibilities in the RMF Process

| Role | | Responsibilities |
|---|---|---|
| | **Information System Owner (ISO) (a.k.a. GCA for government systems and ISSM for contractor-owned systems)** | • Holds responsibility for the procurement, development, integration, modification, operation, maintenance, and disposal of an IS<br>• Addresses the operational interests of the user community and ensures compliance with information security requirements |
| <br> | **Information System Security Manager (ISSM)** | • Serves as a principal advisor on all matters, technical and otherwise, involving the security of an IS under her/his purview<br>• Ensures physical and environmental protection, personnel security, incident handling, and security training and awareness<br>• Monitors a system and its environment of operation to include developing and updating the System Security Plan (SSP), managing and controlling changes to the system, and assessing the security impact of those changes<br>• Must be trained to the level commensurate with the complexity of the contractor's IS or have a local ISSO who is trained. |
| | **Facility Security Officer** | • Supports the ISSM in their efforts to implement security requirements for classified information systems<br>• Ensures physical and environmental protection, personnel security, incident handling, and security training and awareness |
| | **Information System Security Officer (ISSO)** | • If appointed, supports the ISSM in their efforts to implement security requirements as mandated by NISPOM and DAAPM.<br>• Configures and manage the IS configuration |

# RMF Process Walk Through: Introduction

**RMF is a six step process designed to build information security capabilities into Information Systems (IS) throughout the NISP through the application of community best practices for IS management, operational, and technical security controls. The RMF process is explained in further detail in the ISOM and the DAAPM.**


1. Categorize the Information System
2. Select Security Controls
3. Implement Security Controls
4. Assess Security Controls
5. Authorize the Information System
6. Monitor the Information System
Risk Management Framework

# RMF Process Walk Through

**Step 1: Categorize the IS**

- ✓ The ISSM/ISSO categorizes the IS based on the impact due to a loss of confidentiality (moderate/high), integrity (low/moderate/high), and availability (low/moderate/high) of the information or IS according to information provided by the IO.
- ✓ Industry should perform a Risk/Threat Assessment for specific concerns for their Facility/Program.
- ✓ Absent any other requirements Industry may use the DSS baseline of moderate/low/low.
- ✓ The ISSM then documents the description, including the system/authorization boundary in the System Security Plan (SSP)
- ✓ ISSM assign qualified personnel to RMF roles and document team member assignments in the Security Plan

This step will result in the following:

- **Artifact(s):** Risk Assessment and start initial SSP describing the IS Risk(s)
- See NIST SP 800-30 (Risk Assessment) for additional guidance.

1. Categorize the Information
2. Select Security Controls
3. Implement Security Controls
4. Assess Security Controls
5. Authorize the Information System
6. Monitor the Information System
Risk Management Framework

Defense Security Service

# Risk Assessment Report (RAR)

| TYPE OF THREAT SOURCE | DESCRIPTION |
|---|---|
| ADVERSARIAL<br>- Individual (outsider, insider, trusted, privileged)<br>- Group (ad-hoc or established)<br>- Organization (competitor, supplier, partner, customer)<br>- Nation state | Individuals, groups, organizations, or states that seek to exploit the organization's dependence on cyber resources (i.e., information in electronic form, information and communications, and the communications and information-handling capabilities provided by those technologies. |
| ADVERSARIAL<br>- Standard user<br>- Privileged user/Administrator | Erroneous actions taken by individuals in the course of executing everyday responsibilities. |
| STRUCTURAL<br>- IT Equipment (storage, processing, comm., display, sensor, controller)<br>- Environmental conditions<br>o Temperature/humidity controls<br>o Power supply<br>- Software<br>o Operating system<br>o Networking<br>o General-purpose application<br>o Mission-specific application | Failures of equipment, environmental controls, or software due to aging, resource depletion, or other circumstances which exceed expected operating parameters. |
| ENVIRONMENTAL<br>- Natural or man-made (fire, flood, earthquake, etc.)<br>- Unusual natural event (e.g., sunspots)<br>- Infrastructure failure/outage (electrical, telecomm.) | Natural disasters and failures of critical infrastructures on which the organization depends, but is outside the control of the organization. Can be characterized in terms of severity and duration. |

The following tables from the NIST SP 800-30 were used to assign values to likelihood, impact, and risk:

Table 2: Assessment Scale – Likelihood of Threat Event Initiation (Adversarial)

| Qualitative Values | Semi-Quantitative Values | | Description |
|---|---|---|---|
| Very High | 96-100 | 10 | Adversary is **almost certain** to initiate the threat event. |
| High | 80-95 | 8 | Adversary is **highly likely** to initiate the threat event. |
| Moderate | 21-79 | 5 | Adversary is **somewhat likely** to initiate the threat event. |
| Low | 5-20 | 2 | Adversary is **unlikely** to initiate the threat event. |
| Very Low | 0-4 | 0 | Adversary is **highly unlikely** to initiate the threat event |

# RMF Process Walk Through

**Step 2: Select Security Controls**

- ✓ The ISSM (and ISSO, as appropriate) selects the security control baseline applicable to the IS based upon the results of the categorization and tailors the controls as needed by supplementing, modifying, or tailoring out controls to effectively manage risk for any unique system conditions.
- ✓ The ISSM (and ISSO, as appropriate) develops a strategy for continuous monitoring of security control effectiveness.
- ✓ The ISSM then documents the results of selecting the security controls in the SSP via the OBMS.
- ✓ The assigned ISSP/SCA reviews the SSP to ensure it meets the necessary security requirements and effectively identifies potential risks to the IS. The ISSP/SCA also reviews the ISSM-recommended deltas from the standard baseline.
- ✓ The ISSP/SCA then notifies the ISSM of concurrence with selected security controls.

This step will result in the following:

- **Outcome:** Agreed upon security control set.
- **Artifact(s):** Continuous monitoring strategy and updated SSP with controls identified.

1. Categorize the Information
2. Select Security Controls
3. Implement Security Controls
4. Assess Security Controls
5. Authorize the Information System
6. Monitor the Information System
Risk Management Framework

# Security Controls - Overlays

**Table 1: Security Controls for the Overlays**

| Ctrl Nr | Ctrl Name | SUSA | MUSA | A/V | ISOL | |
|---|---|---|---|---|---|---|
| AC-2 | Account Management | | | | | |
| AC-2(1) | Account Management: Automated System Account Management | - | - | - | - | |
| AC-2(2) | Account Management: Removal of Temporary or Emergency Accounts | - | - | - | - | |
| AC-2(3) | Account Management: Disable Inactive Accounts | - | - | - | - | |
| AC-2(7) | Account Management: Role Based Schemes | - | | | | |
| AC-2(9) | RESTRICTIONS ON USE OF SHARED GROUPS / ACCOUNTS | - | | | | |
| AC-2(10) | SHARED / GROUP ACCOUNT CREDENTIAL TERMINATION | - | | | | |
| AC-2(12) | ACCOUNT MONITORING / ATYPICAL USAGE | - | | | | |
| AC-2(13) | DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS | - | | | | |
| AC-3 | Access Enforcement | - | | | | |
| AC-3(2) | DUAL AUTHORIZATION | - | | | | |
| AC-3(4) | Access Enforcement: Discretionary Access Control | - | | | | |
| AC-6(7) | REVIEW OF USER PRIVILEGES | - | | | | |

# SSP Controls

**10.8.1 IA – 1 – Identification and Authentication Policy and Procedures**

Program-specific policies and procedures shall be included in the specific security controls listed below. There is no requirement for the Program to develop additional policy to meet the -1 control.

| **Recommended Continuous Monitoring Frequency: Quarterly** | Program Frequency: | Choose an item. |
|---|---|---|

Implementation Status:

☐ Implemented ☐ Planned

Organizational Tailoring:

☐ Compensatory Control (Provide justification below) ☐ Tailored In (Provide justification below)

☐ Tailored Out (Provide justification below) ☐ Modified (Provide justification below)

Control Origination (check all that apply):

☐ Common ☐ System Specific ☐ Hybrid (Common and System Specific)

The organization:

a. Develops, documents, and disseminates to **all personnel**:

1. An identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

2. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls; and

b. Reviews and updates the current:

1. Identification and authentication policy **at least annually**; and

2. Identification and authentication procedures **at least annually**.

Click here to enter text.

| CONTINUOUS MONITORING STRATEGY | Click here to enter text. |
|---|---|

# RMF Process Walk Through

**Step 3: Implement Security Controls**

- ✓ The ISSM and ISSO implement security controls for the IS and may conduct an initial assessment to facilitate early identification of weaknesses and deficiencies.
- ✓ The ISSM then documents the security control implementation in the Security Controls Traceability Matrix (SCTM) portion of the SSP via the OBMS.

This step will result in the following:

- **Outcome:** Implemented security requirements.
- **Artifact(s):** Updated SSP with a functional description of security control implementation.

1. Categorize the Information
2. Select Security Controls
3. Implement Security Controls
4. Assess Security Controls
5. Authorize the Information System
6. Monitor the Information System
Risk Management Framework

# RMF Process Walk Through

**Step 4: Assess Security Controls - *Part One***

- ✓ The ISSM, with the ISSO, develops a Security Assessment Plan (SAP) that addresses objectives for the assessment, methods for verifying security control compliance, the schedule for the initial control assessment, and actual assessment procedures. *(Cleared Industry can leverage assessment procedures in the DAAPM).*
- ✓ The ISSM then conducts the initial assessment of the effectiveness of the security controls and documents the issues, findings, and recommendations in a Security Assessment Report (SAR).
- ✓ The ISSM, after the initial assessment, conducts remediation actions based on the findings and recommendations in the Plan of Action and Milestones (POA&M), signs a Certification Statement, and submits the SSP (using the OBMS) to DSS.

Risk Management Framework
Categorize the Information
2. Select Security Controls
3. Implement Security Controls
4. Assess Security Controls
5. Authorize the Information System
6. Monitor the Information System

# RMF Process Walk Through

**Step 4: Assess Security Controls - *Part Two***

- ✓ The ISSP/SCA receives the SSP, performs an SSP review, and conducts an on-site validation/assessment.
- ✓ The ISSP/SCA informs the ISSM of any additional deficiencies or weaknesses discovered and identifies necessary remediation actions in a POA&M.
- ✓ The ISSP/SCA schedules a revalidation visit if necessary and makes final updates to the SAR.

This step will result in the following:

- **Outcome:** Tested, evaluated, and remediated security controls.
- **Artifact(s):** SAR, and final SSP.

**Additional guidance for assessing controls: NIST SP 800-53A**

1. Categorize the Information
2. Select Security Controls
3. Implement Security Controls
4. Assess Security Controls
5. Authorize the Information System
6. Monitor the Information System
Risk Management Framework

# RMF Process Walk Through

**Step 5: Authorize the IS**

- ✓ The ISSP/SCA reviews and submits the security authorization package to the DAO.
- ✓ The DAO assesses the security authorization package and issues an authorization decision for the IS—either Authorization to Operate (ATO) or Denied Authorization to Operate (DATO)—which includes any terms and conditions of operation as well as the authorization termination date (ATD).

This step will result in the following:

- **Outcome:** Risk determination and acceptance decision by the DAO.
- **Artifact(s):** Complete security authorization determination to include the POA&M.

1. Categorize the Information
2. Select Security Controls
3. Implement Security Controls
4. Assess Security Controls
5. Authorize the Information System
6. Monitor the Information System
Risk Management Framework

# RMF Process Walk Through

**Step 6: Monitor the IS**

- ✓ The ISSM determines the security impact of proposed or actual changes to the IS and its operating environment and informs the ISSP/SCA as necessary.
- ✓ The ISSM assesses a selected subset of the security controls, based on the approved continuous monitoring strategy, and informs the ISSP/SCA of the results.
- ✓ The ISSM updates SSP documentation and works to satisfy POA&M requirements, and provides regular status reports to their ISSP/SCA per the continuous monitoring strategy.
- ✓ The ISSM conducts any necessary remediation actions based on findings discovered during continuous monitoring.
- ✓ The ISSM ensures IS security documentation is updated and maintained and reviews the reported security status of the IS.
- ✓ As necessary, the ISSM develops and implements an IS decommissioning strategy.

This step will result in the following:

- **Outcome:** Continued evaluation and remediation of the authorized IS.
- **Artifact(s):** Updated POA&M, updated SSP, and decommissioning strategy (as necessary).

Categorize the Information
2. Select Security Controls
3. Implement Security Controls
4. Assess Security Controls
5. Authorize the Information System
6. Monitor the Information System
Risk Management Framework

# Security Controls and Continuous Monitoring

The RMF process will manage risk more effectively through the introduction of security controls and continuous monitoring of those controls.

| Purpose of Security Controls and Continuous Monitoring | Benefits of Security Controls and Continuous Monitoring |
|---|---|
| ✓ Assess security control effectiveness for an IS<br>✓ Document changes to the IS or its environment of operation<br>✓ Conduct security impact analyses of associated changes<br>✓ Report the security status of an IS | ✓ Facilitate more efficient enterprise management of cybersecurity<br>✓ Increase security in the system development and acquisition processes<br>✓ Ensure compliance with national standards and reporting requirements |

**Resources to assist in the RMF Process**

Many additional resources can be found on the NIST website (www.nist.gov )

- **National Industrial Security Program Operating Manual (NISPOM)**
- **NIST SP 800-37:** Guide for Applying the Risk Management Framework to Federal Information Systems
- **NIST SP 800-137:** Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
- **NIST SP 800-53:** Security and Privacy Controls for Federal Information Systems and Organizations
- **NIST SP 800-53A:** Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans
- **Committee on National Security Systems Instruction (CNSSI) 1253:** Security Categorization and Control Selection for National Security Systems

# Transition Timeline

| System Accreditation Status | Transition Timeline / Instructions |
|---|---|
| | Continue using current C&A process with the latest version of the ODAA Process Manual. The ATO will last no greater than 18 months starting October 3, 2016. Within six months of authorization, develop a Plan of Action and Milestones (POA&M) for transition to RMF. |
| **SSPs/MSSPs after October 3, 2016.** | Execute RMF Assessment and Authorization through the DAAPM.<br><br>Standalones are no longer allowed to be self-certified under the C&A process. |
| | **Phase 1:** Cleared contractors continue using the current C&A process with the latest version of the ODAA Process Manual. ATO will last no greater than 18 months starting October 3, 2016. Within six months of authorization, develop a POA&M for transition to RMF.<br><br>**Phase 2:** Execute RMF Assessment and Authorization process through the DAAPM. *(Timeline TBD.)* |

# Resources

CDSE Training courses

- Introduction to RMF (CS124.16)
- Continuous Monitoring (CS200.16)
- Categorization of the System (CS102.16)
- Selecting Security Controls (CS103.16)
- Implementing Security Controls (CS104.16)
- Assessing Security Controls (CS105.16)
- Authorizing Systems (CS106.16)
- Monitoring Security Controls (CS107.16)

- www.dss.mil/rmf